FIPS Physical security workshop, Hawaii 2005

Introduction to side channel attacks and non invasive attacks

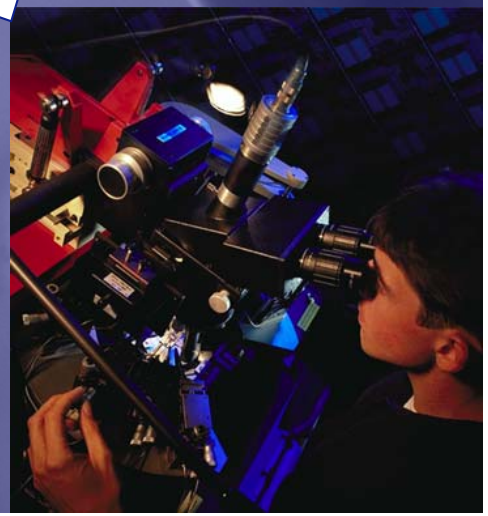
TNO ITSEF

Jan Blonk

TNO ITSEF

www.itsef.com

Blonk@itsef.com



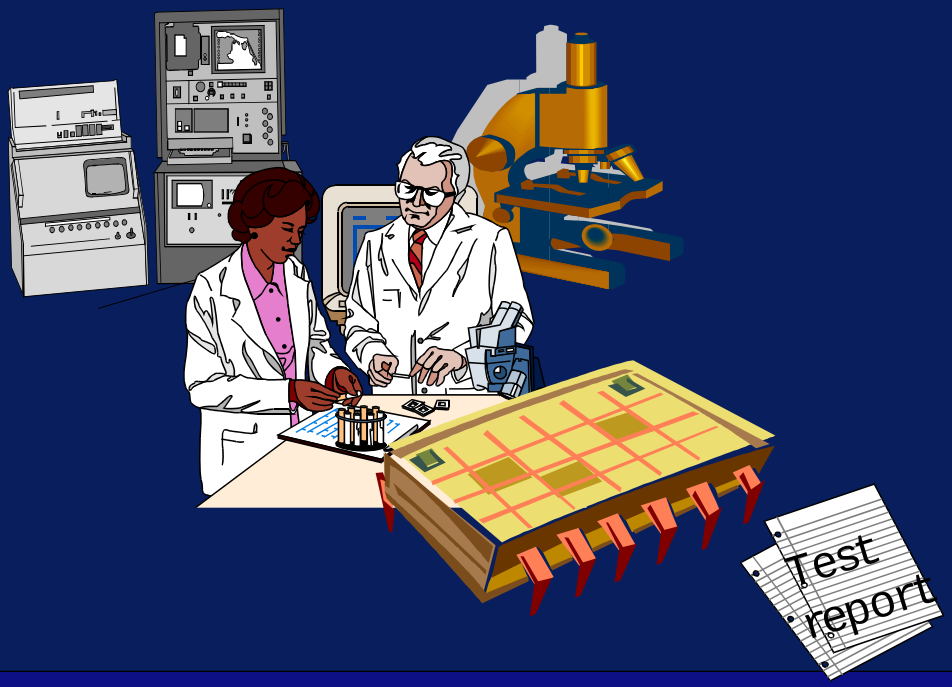
TNO ITSEF

"IT Security Evaluation Facility"

- TNO is an independent R&D company in the Netherlands
- TNO ITSEF is owned by TNO
- TNO ITSEF provides services for:
  - -security evaluations
  - -developer support services
- strict procedures for maintaining client secrecy of sensitive information

Chip security evaluations

TNO ITSEF performs chip evaluations according to different schemes (VISA, MasterCard, CC)

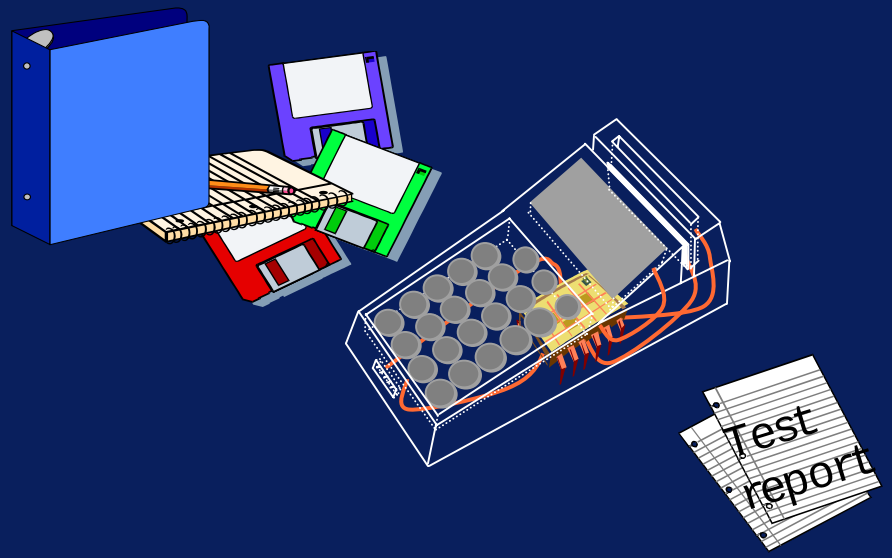


Smart Card security evaluations

TNO ITSEF performs formal and informal evaluations on smart cards with GlobalPlatform or proprietary OSs according to different schemes (VRIR, CAST, CC, other)

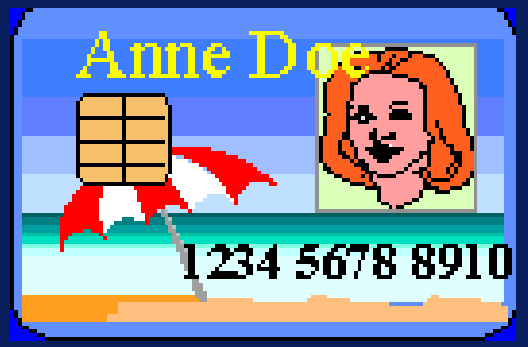
Terminal security evaluations

TNO ITSEF performs formal and informal security evaluations on payment terminals according to different schemes (PCI/PED, CC, other)



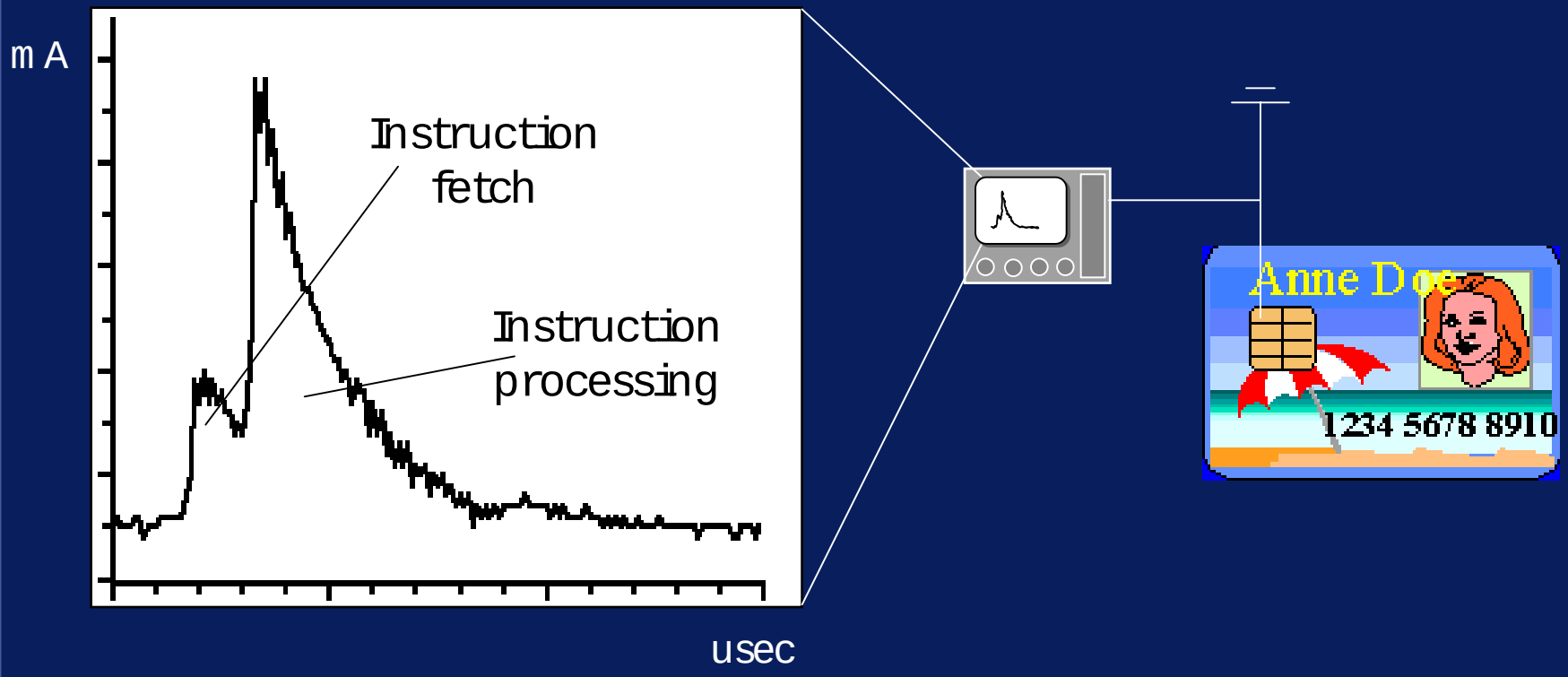
Smart cards

- Side channel attacks
  - SPA/DPA
  - EMA/DEMA
- Perturbation
  - Light flashes
  - Voltage glitches
  - Excess conditions
    - Frequency
    - Voltage
    - temperature
    - reset
    - light
    - (radiation)



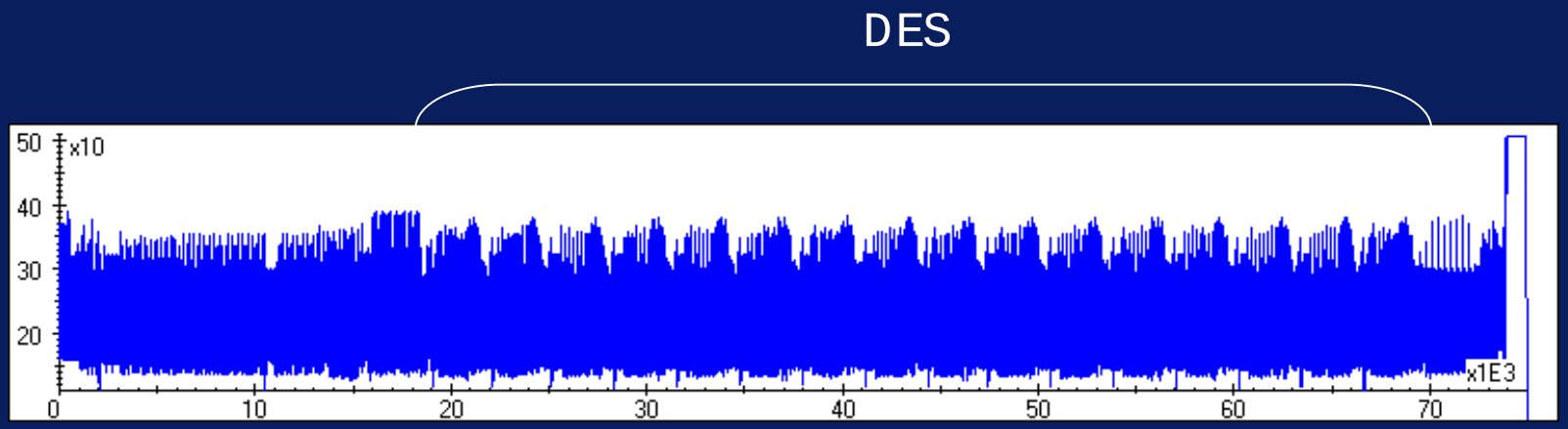
Power analysis

Power leakage



Power consumption trace

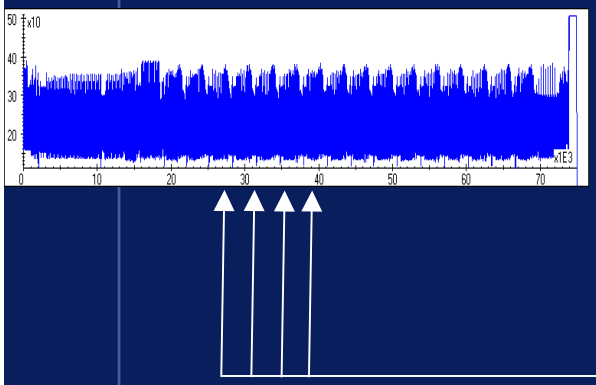
- 5-10000 clock cycles (instructions)
- Characteristic structures become visible

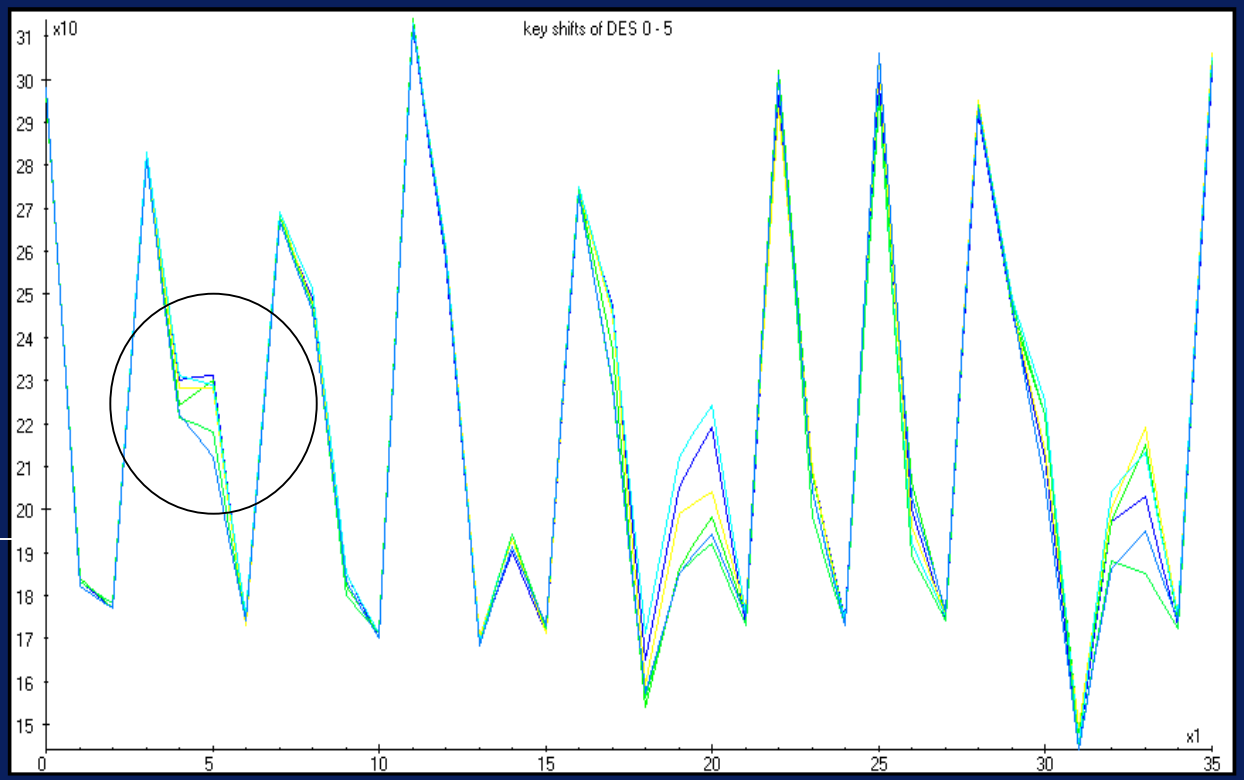


Power consumption dependent on data bits

Simple power analysis:

Recognise differences in power consumption for “0” and “1” databits

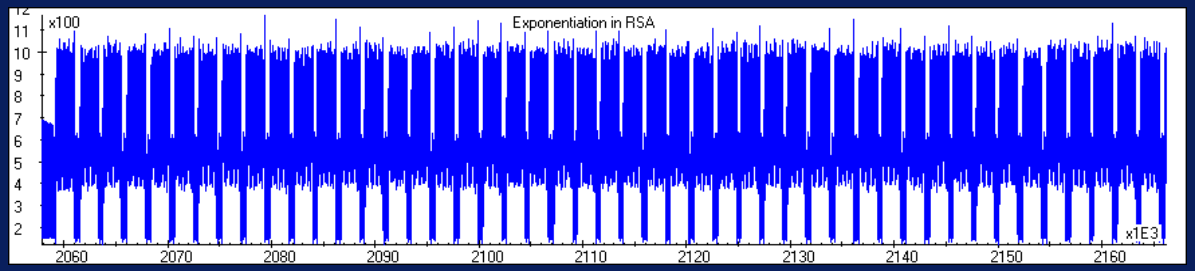


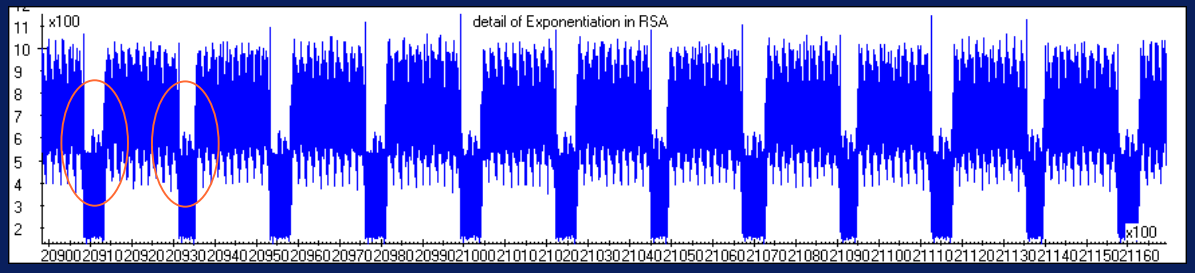


Timing dependent on data bits

Simple Power Analysis

Example of timing attack on RSA



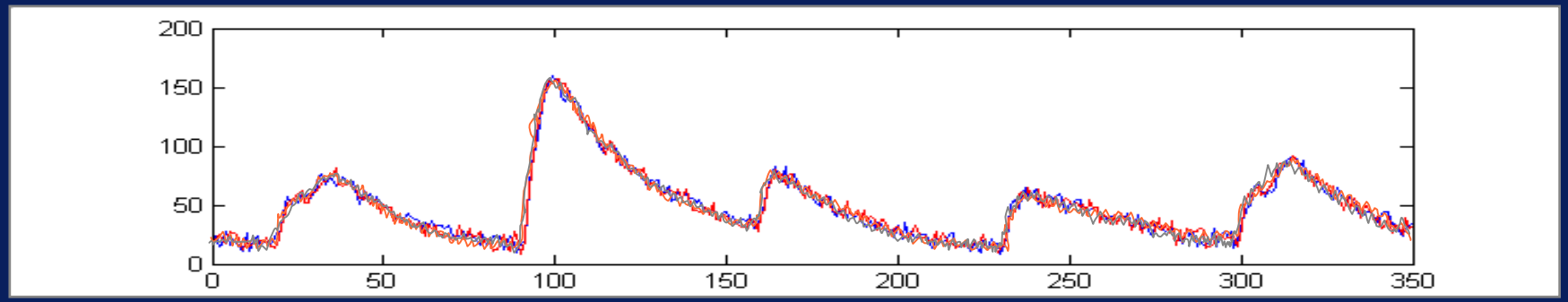


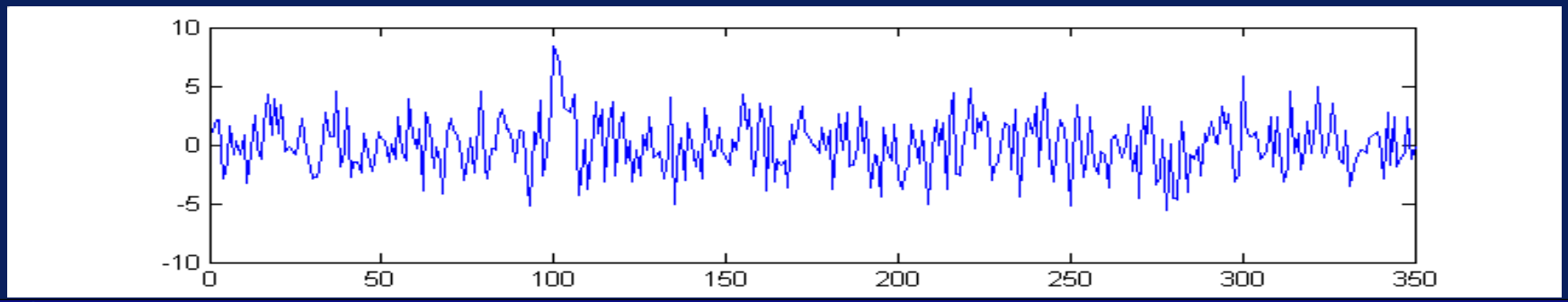
1 0 0 0 1 1 1

Principles of DPA

Large amount of traces:

- Assume power consumption relates to hamming weight of data
- Subtract traces with high and low hamming weight
- Resulting trace shows hamming weight and data manipulation





DPA countermeasures

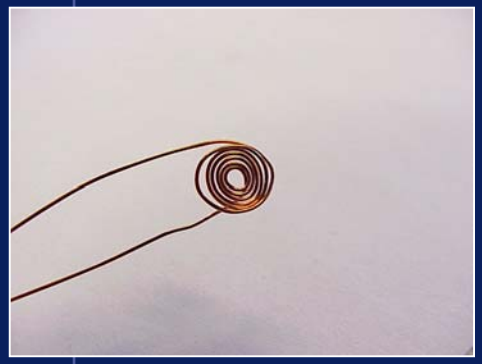
Protection against DPA is a combination of:

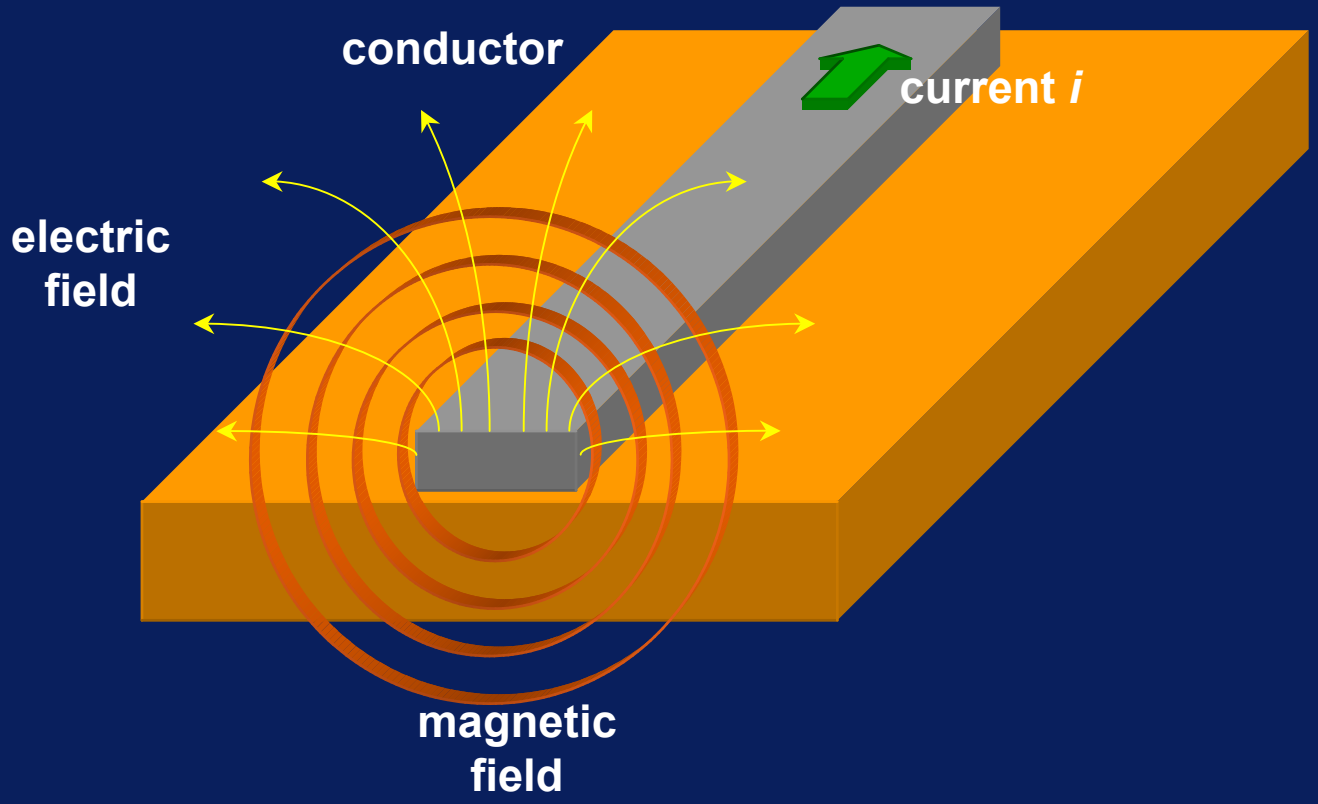
- Hardware
  - signal reduction
  - adding amplitude noise
  - adding timing noise
  - Dedicated components
- Software
  - Time constant programming
  - Adding random delays or alternating paths
  - blinding of intermediate values with random values

Set up for power analysis

Electromagnetic fields

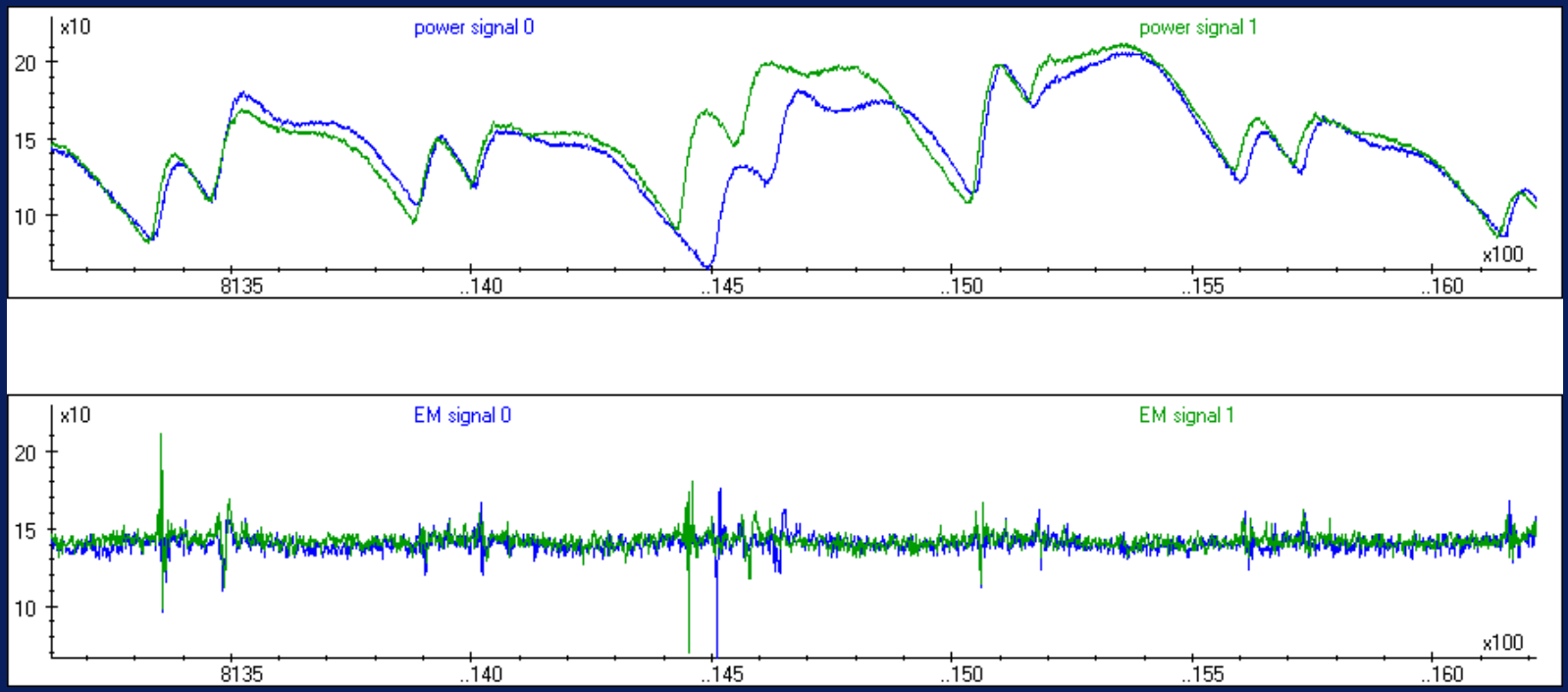
Principles of EMA





EM signals

Same information content as power signals



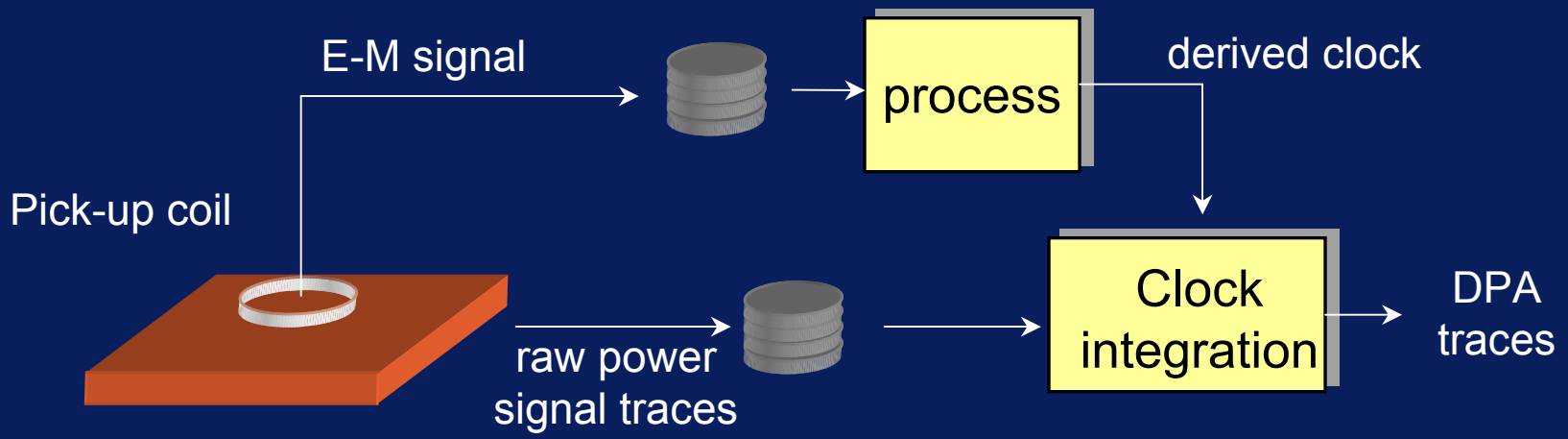
DPA and DEMA countermeasures

Protection against DPA and DEMA is a combination of:

- Hardware
  - signal reduction
  - adding amplitude noise
  - adding timing noise
  - Dedicated components
- Software
  - Time constant programming
  - Adding random delays or alternating paths
  - blinding of intermediate values with random values

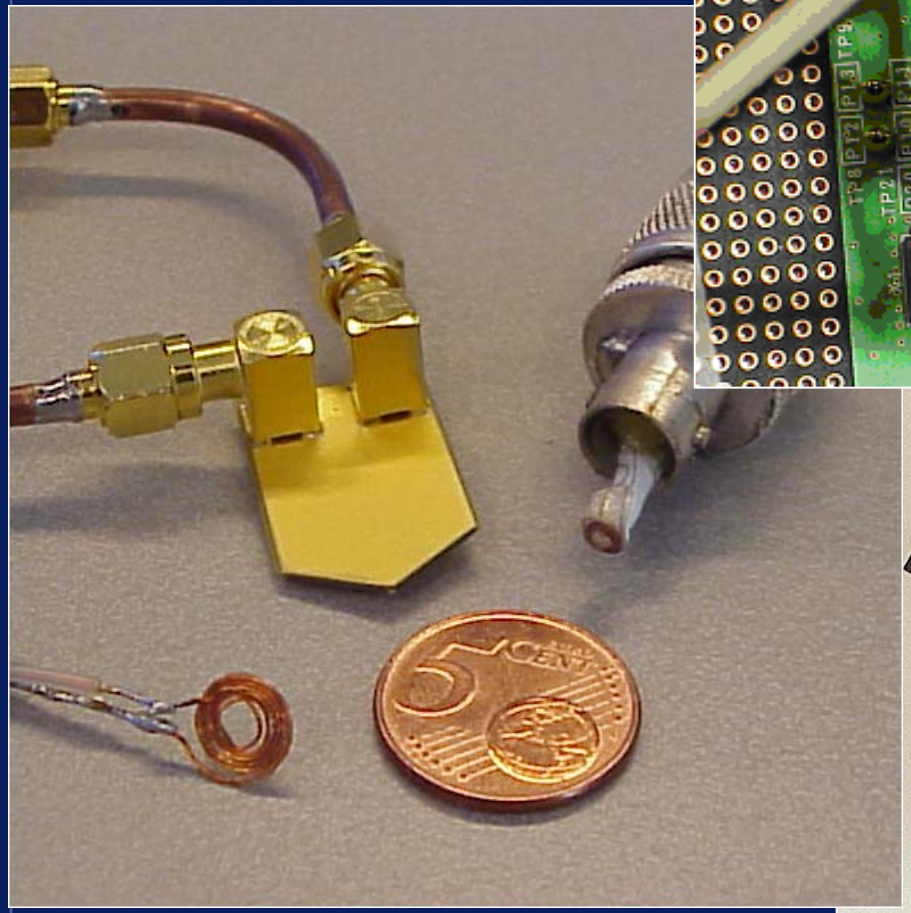
Added EM value

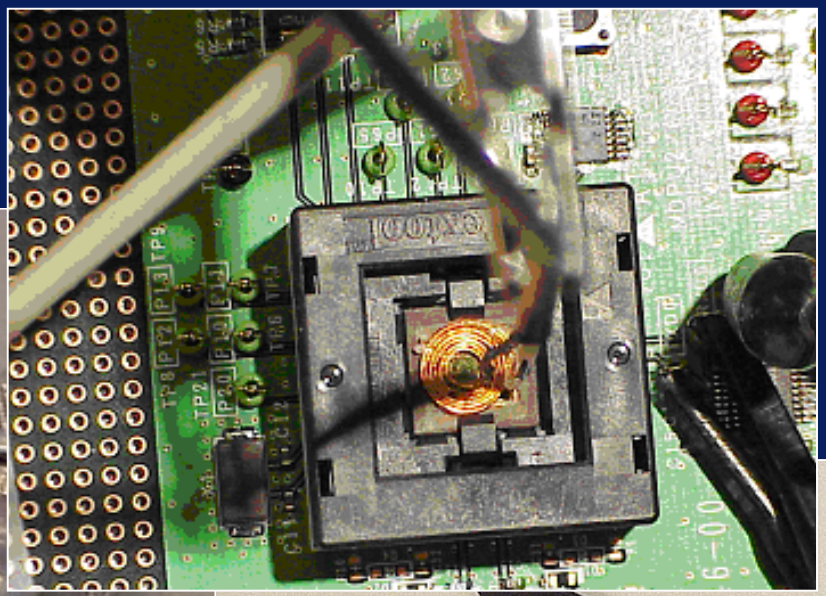
- Aid for reverse engineering: locate functional blocks
- Multi-channel Analysis:
  Clock extraction for re-alignment of power traces

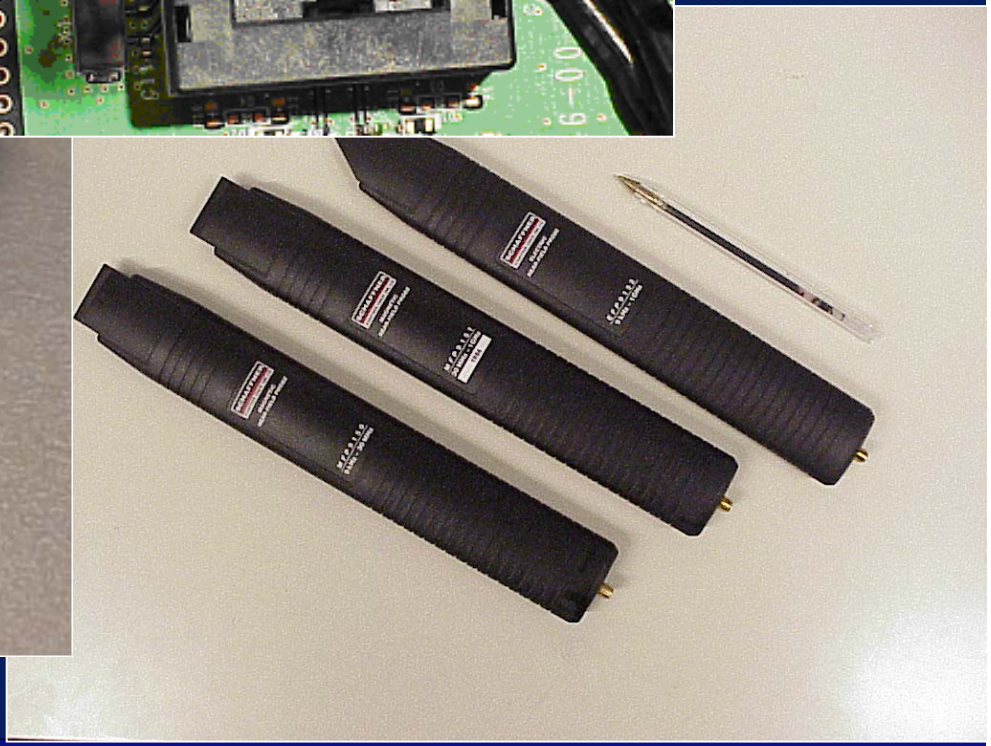


- Also applicable for terminals, phones, PDA's

Coils for EM A



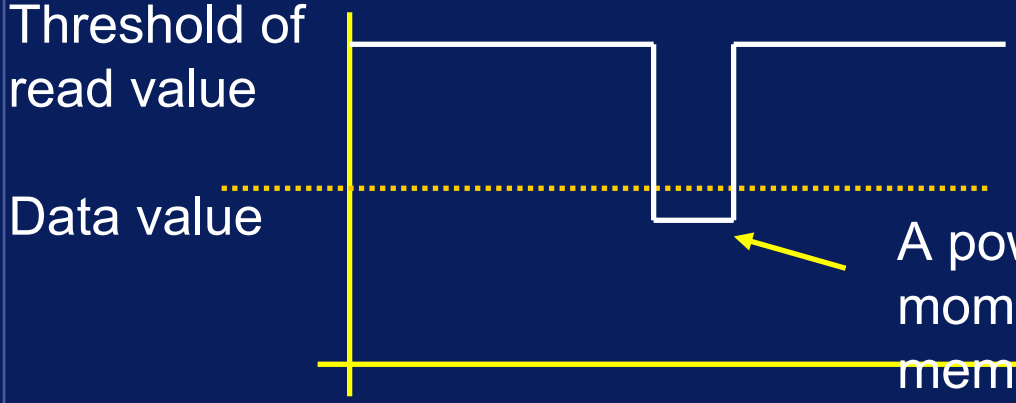




Non invasive attacks (perturbation)

Voltage Glitching:

- Very short glitches on the supply voltage
- Can change the value of read data



Voltage glitch attack

- Select target

Changing calculations:

2A + 2B = 200

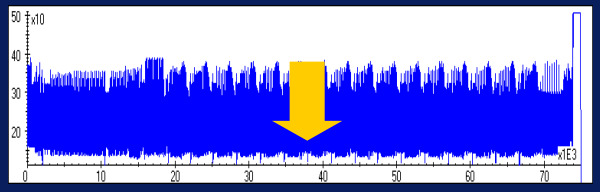
2A + 0B = 100

=> A= 50

Changing program flow:

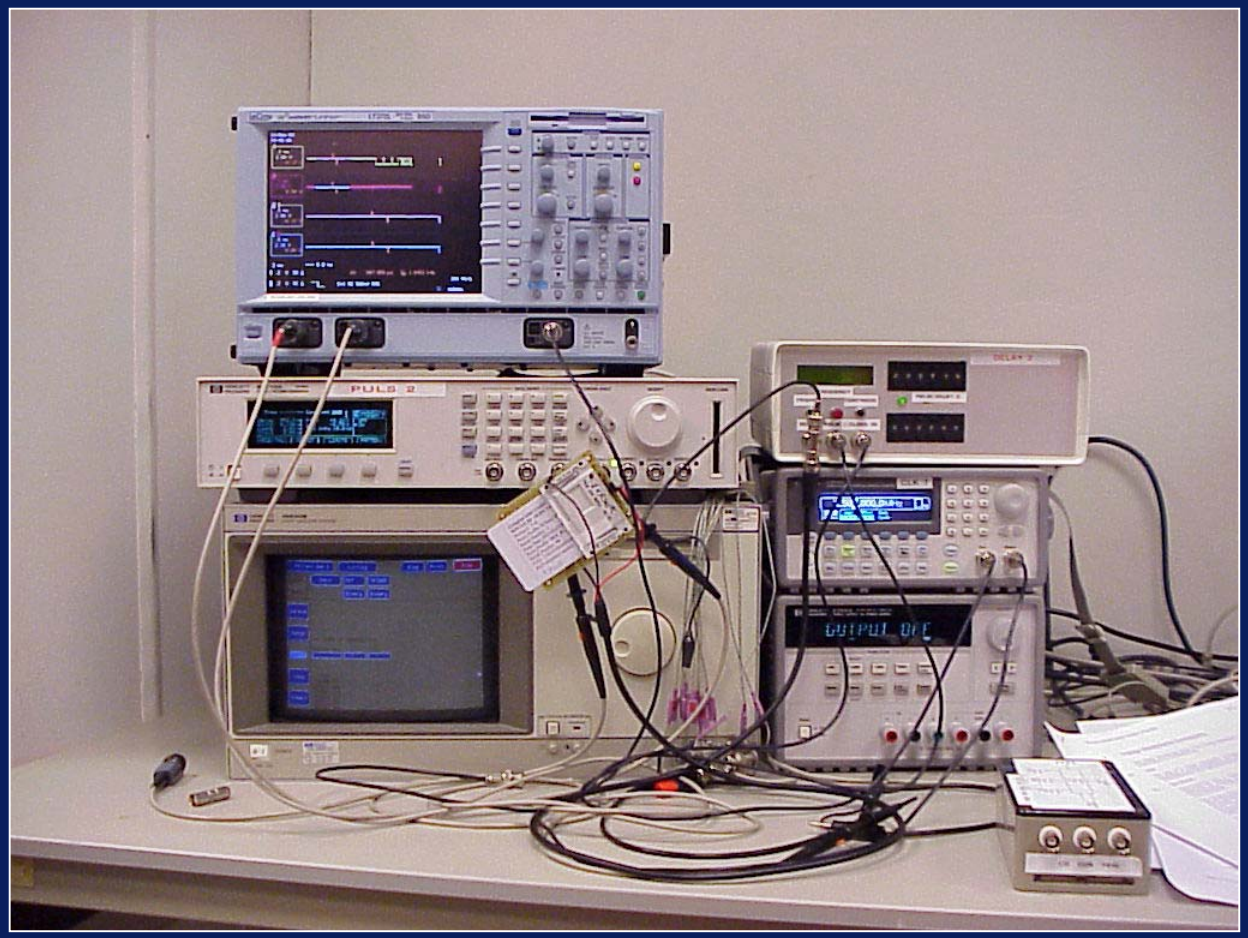
```
Result = Verify(PIN)
IF result > 0
THEN Authorize()
END
```

- Determine timepoint



- Administer glitch

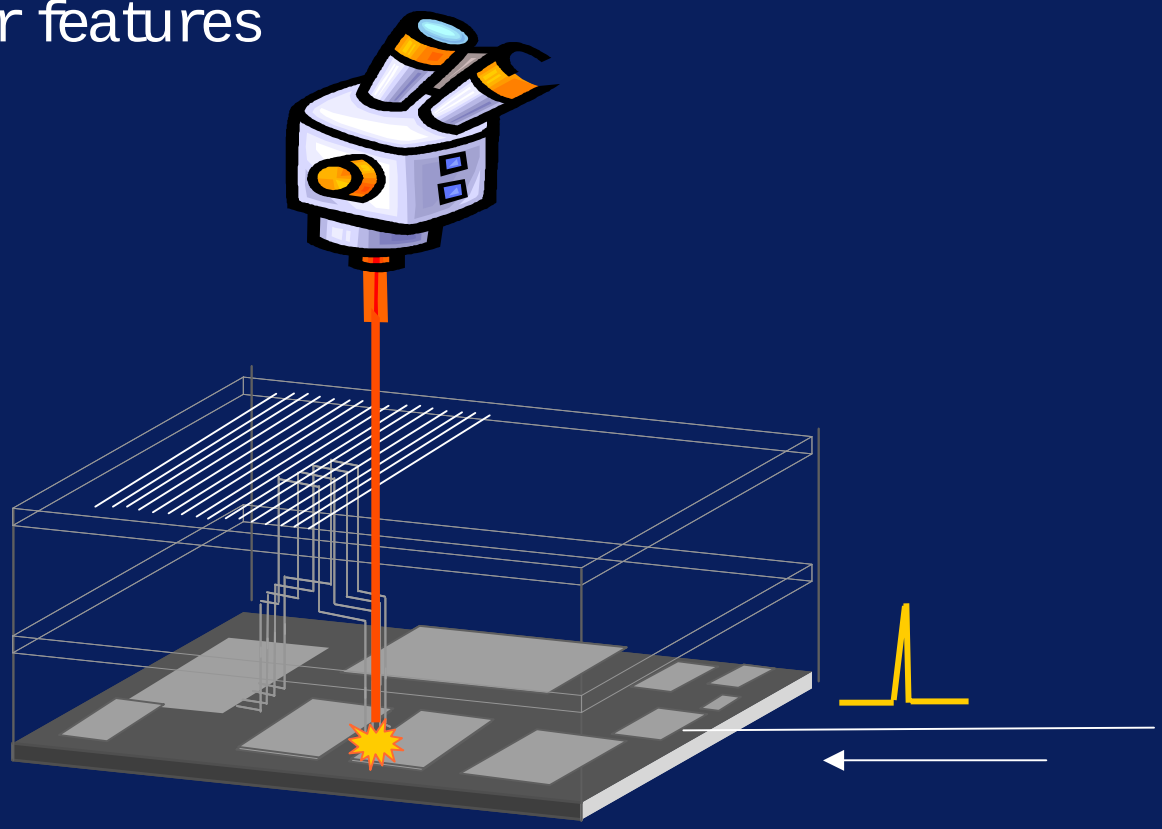
Example of voltage glitch setup



Light attack

Added value:

- Can target smaller features in the chip



Example of light attack set up